

1 IAP20 Rec'd PCT/PTO 20 DEC 2005

Description

DÉCODEUR ET SYSTÈME DESTINÉ AU TRAITEMENT DE DONNÉES DE TÉLÉVISION À PÉAGE ET PROCÉDÉ POUR LA GESTION D'AU MOINS DEUX DÉCODEURS

- [1] La présente invention concerne un décodeur destiné au traitement de données de télévision à péage. Elle concerne également un système de gestion de données de télévision à péage ainsi qu'un procédé de gestion d'au moins deux décodeurs destinés au traitement de données de télévision à péage.
- [2] Généralement, pour pouvoir accéder à un contenu chiffré correspondant à des événements diffusés par des opérateurs de télévision à péage, tels que des films, des matchs de sports ou autre, il faut acquérir un abonnement, un décodeur et un module de sécurité. Certains abonnés souhaitent disposer de plusieurs décodeurs et de plusieurs modules de sécurité pour que plusieurs utilisateurs puissent accéder aux événements diffusés à partir de plusieurs téléviseurs disposés dans des pièces différentes de leur habitation.
- [3] Dans ce cas, le prix demandé pour les abonnements, décodeurs et/ou modules de sécurité ultérieurs est généralement inférieur au prix demandé pour le premier abonnement, décodeur et/ou module de sécurité. On cherche toutefois à éviter qu'un abonné n'acquière plusieurs ensembles décodeurs/modules de sécurité, en bénéficiant de la réduction de prix pour les ensembles ultérieurs et qu'il fasse bénéficier un tiers non abonné de cette réduction ou revende ces ensembles à un prix plus bas que le prix d'acquisition normal.
- [4] Une solution pour éviter ceci consiste à imposer une manipulation qui est peu contraignante pour un abonné qui dispose réellement de plusieurs décodeurs associés aux modules de sécurité dans son logement, mais qui est par contre très contraignante pour un abonné qui a revendu les décodeurs et les modules de sécurité ou pour l'acheteur de tels modules. De plus, si cette manipulation n'est pas effectuée, les fonctions de déchiffrement du contenu transmis ne sont pas possibles.
- [5] Un système permettant d'atteindre en partie ce but est décrit dans le brevet européen publié sous le numéro EP 0 826 288. Ce brevet décrit un système de télévision à péage comprenant plusieurs ensembles de télévisions, chaque ensemble étant lié à un abonné spécifique. Chaque ensemble est formé d'au moins deux décodeurs, chaque décodeur étant associé à une carte à puce destinée à permettre le déchiffrement du contenu envoyé sur les décodeurs liés au système de télévision. Chaque carte à puce contient un certain nombre d'informations qui permettent de l'identifier. Ces informations, appelées 'données de chaînage', sont par exemple une signature, une clé ou un autre élément de détermination. Toutes les cartes liées au même abonné ont au moins une des données de chaînage en commun. Des cartes d'abonnés différents n'ont pas de données en commun.

- [6] Les cartes à puce de l'abonné, ou au moins l'une d'entre elles, peuvent être désactivées selon des critères prédéfinis. Ces critères peuvent par exemple être une date déterminée ou une durée d'utilisation. Lorsqu'une carte est désactivée, les mots de contrôle ne sont plus déchiffrés. Le contenu envoyé sur le décodeur considéré ne peut plus être déchiffré sans ces mots de contrôle correspondant à des événements diffusés.
- [7] Une carte désactivée peut être réactivée si l'abonné dispose d'une carte encore active et d'un décodeur lié au même abonné. Pour réaliser ceci, le système selon cette invention de l'art antérieur fonctionne de la manière suivante.
- [8] Les données liées à une carte active sont tout d'abord mémorisées dans le décodeur dans lequel cette carte est introduite. Lorsqu'une carte est désactivée, elle doit être introduite dans un décodeur associé à une carte active de l'abonné. Les données de chaînage telles que la signature, la clé, etc., mémorisées dans le décodeur, sont authentifiées avec les données de chaînage de la carte désactivée. Si ces données concordent, le compteur contenant par exemple la date prochaine de désactivation ou la durée d'utilisation est incrémenté de façon à permettre l'utilisation de la carte pendant un certain temps. Si ces données de chaînage ne concordent pas, le compteur n'est pas réinitialisé dans la carte désactivée, le déchiffrement des mots de contrôle n'est pas possible et l'événement reste chiffré.
- [9] Dans ce système, n'importe quel décodeur lié à une carte active de l'abonné peut permettre de réactiver une carte désactivée si les données de chaînage correspondent, c'est-à-dire si elles appartiennent au même abonné. De ce fait, si des cartes de l'abonné ont été vendues à des personnes géographiquement proches de l'abonné initial, les personnes qui ont une carte désactivée peuvent introduire cette carte dans n'importe quel décodeur lié à une carte active de l'abonné pour refaire fonctionner la leur. L'effet dissuasif recherché par l'invention n'est donc que partiellement atteint.
- [10] Il existe en outre une manière simple d'éviter les contraintes liées au procédé de ce brevet. Il suffit en effet que l'acheteur d'un ensemble décodeur/carte à puce non autorisé acquiert deux ensembles. Ainsi, il pourra toujours réactiver une carte lorsque celle-ci sera désactivée.
- [11] Un autre problème arrive lorsque toutes les cartes sont désactivées. Ceci peut se produire notamment lorsqu'un abonné ne regarde que rarement la télévision ou qu'il est absent entre le moment où la première carte est désactivée et le moment où la dernière est désactivée. Dans ce cas, il n'est plus possible de réactiver une carte et la seule solution consiste à commander une autre carte.
- [12] Dans l'invention décrite dans cette publication EP 0 826 288, toutes les informations importantes, c'est-à-dire essentiellement les données de chaînage et les données relatives à la date de désactivation sont mémorisées dans la carte. Les décodeurs jouent uniquement un rôle de 'mémoire tampon' pour transférer les informations de chaînage entre une carte active et une autre carte désactivée lors de la procédure de réactivation.

- [13] Une autre invention permettant d'atteindre le but mentionné ci-dessus est décrit dans la publication US 5 748 732. Ce document concerne un système de télévision à péage comportant un décodeur maître et un ou plusieurs décodeurs esclaves, munis de cartes à puce. Les cartes à puce des décodeurs esclaves ont une durée de validité limitée, relativement courte, ce qui signifie qu'ils ne peuvent plus déchiffrer des données chiffrées lorsque la durée de validité est écoulée. Afin de réactiver une carte à puce dont la durée de validité est écoulée, un centre de gestion envoie un message d'autorisation EMM au décodeur maître. Celui-ci le traite de façon à en extraire les nouvelles données de fonctionnement de la carte à puce esclave. Ces données sont mémorisées dans le décodeur maître. Lorsque l'utilisateur souhaite réactiver sa carte esclave, il doit l'introduire dans le décodeur maître qui transfère les données mémorisées à cette carte. Elle pourra de nouveau fonctionner lors de son introduction dans le décodeur esclave.
- [14] Dans cette réalisation, comme précédemment, toutes les données importantes et en particulier les données relatives à la durée de fonctionnement des cartes esclaves sont mémorisées dans les cartes elles-mêmes. Le décodeur maître joue uniquement un rôle de 'mémoire tampon' pour transférer les informations de réactualisation depuis la carte maître à une carte esclave. En particulier, ce décodeur ne comporte pas de compteur capable de gérer la durée d'activation d'une carte.
- [15] La présente invention se propose d'offrir une solution alternative assurant une sécurité et un contrôle de l'accès aux événements envoyés par l'opérateur. Elle a pour but de permettre la gestion de façon souple, de la durée de fonctionnement d'un décodeur et d'adapter les paramètres de fonctionnement par le module de sécurité à tout instant.
- [16] Le dispositif a pour but en outre de gérer chaque abonné de façon globale. Ainsi, un abonné qui revend un ou plusieurs ensembles décodeur/module de sécurité se verra imputer les factures des événements consommés par les utilisateurs de ces ensembles. Ceci augmente fortement l'effet dissuasif recherché dans cette invention.
- [17] De plus, l'invention permet également de collecter et de gérer des informations fournies par les ensembles décodeur/module de sécurité, comme par exemple des informations de service ou les données relatives à l'achat impulsif d'événements, aussi bien du point de vue de la facturation que du point de vue des statistiques.
- [18] Les buts de l'invention sont atteints par un décodeur destiné au traitement de données de télévision à péage, ce décodeur étant associé à au moins un module de sécurité amovible au moyen de données d'identification contenues dans ledit décodeur et dans le module de sécurité, ce décodeur comportant un module de désembrouillage, le décodeur étant caractérisé en ce qu'il comporte en outre des moyens de désactivation du traitement des données de télévision à péage et un compteur agissant sur lesdits moyens de désactivation en fonction de son contenu.
- [19] Ces buts sont également atteints par un système de gestion de données de

télévision à péage comportant au moins deux décodeurs, chaque décodeur étant associé à au moins un module de sécurité amovible au moyen de données d'identification contenues dans ledit décodeur et dans ledit module de sécurité, ces décodeurs comportant un module de désembrouillage et des moyens de désactivation du traitement des données de télévision à péage, ce système étant caractérisé en que les décodeurs contiennent en outre un compteur agissant sur lesdits moyens de désactivation, et en ce qu'au moins un des modules de sécurité est déclaré maître et comprend des moyens pour réinitialiser lesdits compteurs des décodeurs.

- [20] Ces buts sont en outre atteints par un procédé de gestion d'au moins deux décodeurs destinés au traitement de données de télévision à péage, lesdits décodeurs étant associés à un abonné et comportant des moyens de désactivation du traitement des données de télévision à péage et un compteur agissant sur lesdits moyens de désactivation, chaque abonné disposant d'au moins deux modules de sécurité amovibles pouvant être localement connectés à au moins un décodeur, ce procédé comprenant les étapes de :
- [21] - détermination d'au moins un module de sécurité maître parmi les modules de sécurité appartenant à un abonné,
- [22] - mémorisation dans chaque décodeur de l'abonné, de données d'identification du module de sécurité maître,
- [23] - désactivation par le compteur du décodeur du traitement des données selon au moins un critère prédéfini,
- [24] - réinitialisation du compteur par l'introduction du module de sécurité maître dans le décodeur désactivé.
- [25] L'invention sera mieux comprise grâce à la description détaillée qui va suivre et qui se réfère aux dessins annexés donnés à titre d'exemples nullement limitatifs, dans lesquels:
- [26] - la figure 1 illustre les éléments placés chez un abonné d'une part et ceux placés chez un diffuseur d'événements de télévision à péage d'autre part;
- [27] - la figure 2a est un schéma bloc représentant les opérations liées à l'activation d'un premier décodeur, selon un premier mode de réalisation;
- [28] - la figure 2b est un schéma bloc représentant les opérations liées à l'activation d'un deuxième décodeur pour un même abonné, selon le mode de réalisation de la figure 2a;
- [29] - La figure 3 est un schéma bloc représentant une partie du fonctionnement du dispositif de l'invention;
- [30] - la figure 4a est un schéma bloc représentant les opérations liées à l'activation d'un premier décodeur, selon un deuxième mode de réalisation;
- [31] - la figure 4b est un schéma bloc représentant les opérations liées à l'activation d'un deuxième décodeur pour un même abonné, selon le mode de réalisation de la figure 4a;
- [32] - La figure 5 représente le système selon l'invention, fonctionnant d'après un troisième mode de réalisation;

- [33] - la figure 6a est un schéma bloc représentant les opérations liées à l'activation d'un premier décodeur, selon un troisième mode de réalisation, également illustré par la figure 5;
- [34] - la figure 6b est un schéma bloc représentant les opérations liées à l'activation d'un deuxième décodeur pour un même abonné, selon le mode de réalisation de la figure 6a;
- [35] - Les figures 7a, 7b, 7c et 7d représentent des architectures possibles du dispositif selon l'invention.
- [36] L'invention est décrite ci-dessous en référence à plusieurs modes de réalisation, dans lesquels il est supposé que l'abonné dispose de plusieurs décodeurs STB1, STB2, STB3,... chacun d'eux étant associé à un module de sécurité ICC1, ICC2, ICC3,..., qui peut par exemple être réalisé sous la forme d'une carte à microprocesseur ou carte à puce ou sous la forme d'un boîtier de circuit intégré. Les décodeurs comportent chacun un module de désembrouillage agencé pour traiter les données chiffrées et permettre leur utilisation en clair, une mémoire destinée à mémoriser des données d'identification, et des moyens de désactivation agencés pour autoriser ou interdire l'accès aux données de télévision à péage.
- [37] Selon une première forme de réalisation illustrée par les figures 2a et 2b, lorsque l'utilisateur acquiert un premier contrat d'abonnement de télévision à péage, C1, ce qui est illustré par une étape 20 sur la figure 2a, il acquiert également un premier décodeur STB1 associé à un premier module de sécurité ICC1. Ceci est illustré par la référence 21 de la figure 2a. De façon bien connue de l'homme du métier, le module de sécurité gère les droits associés aux événements ainsi que le renvoi de mots de contrôle au décodeur de façon à permettre à celui-ci de traiter les données de télévision à péage et par conséquent, de décoder le contenu chiffré lié à un événement.
- [38] Lorsque l'abonné a acquis l'ensemble des éléments nécessaires au décodage d'événements, c'est-à-dire un abonnement, un décodeur et un module de sécurité, il doit en premier lieu, activer ces éléments de façon à les rendre fonctionnels. Sans cette activation, l'ensemble n'est pas en mesure de traiter les données de télévision à péage.
- [39] Selon une forme de réalisation concrète, lorsque l'abonné souhaite activer son décodeur STB1 et son module de sécurité ICC1 pour la première fois, il doit appeler un centre de gestion CG et indiquer des données d'identification, en particulier un numéro d'identification C1 lié à son contrat d'abonnement, un numéro d'identification unique SN_i lié au module de sécurité, un numéro d'identification unique SN_d lié au décodeur et éventuellement son nom (Sub1, Sub2) à des fins de vérification. Ceci est illustré par la référence 22 de la figure 2a. Les numéros d'identification sont également couramment appelés numéros de série. Ces opérations sont généralement réalisées par l'opérateur installant le système chez l'abonné.
- [40] Ces informations seront utilisées par le centre de gestion pour enregistrer l'abonné (Sub1, Sub2), en liaison avec le décodeur STB et le module de sécurité ICC qu'il a acquis et pour apparier le décodeur et le module de sécurité. Il est à noter que le

décodeur et le module de sécurité peuvent être acquis séparément, de sorte qu'avant l'appel au centre de gestion, celui-ci n'a pas de moyens de savoir quel module de sécurité est associé à un décodeur déterminé.

- [41] Comme cela est illustré sous la référence générale CG de la figure 1, le centre de gestion contient au moins une base de données dans laquelle sont mémorisées des informations permettant de lier le module de sécurité au décodeur. De façon plus détaillée, le centre de gestion contient, dans sa base de données, le numéro d'identification unique SN_d de chaque décodeur STB géré par ce centre. Ce numéro unique est associé à au moins une clé de chiffrement U_k (de type symétrique ou asymétrique) qui est différente pour chaque décodeur. Cette clé de chiffrement, dénommée 'clé d'appariement' est également mémorisée dans le décodeur lui-même. Lorsque l'abonné a identifié son décodeur au moyen du numéro unique SN_d et qu'il a indiqué le numéro unique SN_s du module de sécurité, le centre de gestion associe, dans la base de données, le module de sécurité au décodeur. Dans la figure 1, le contenu de la base de données est représenté sous la forme de trois tableaux. L'un des tableaux 15 contient la liste de tous les décodeurs STB gérés par le centre de gestion, associés à leur numéro d'identification unique ainsi qu'à leur clé d'appariement U_k . Un autre tableau 16 contient la liste de tous les modules de sécurité ICC ainsi que leur numéro d'identification unique SN_s . Le troisième tableau 17 contient la liste des contrats d'abonnement C1, C2, ... et des abonnés Sub1, Sub2, ... associés chacun à leurs décodeurs STB d'une part et leurs modules de sécurité ICC d'autre part. Ce tableau contient également la liste des produits P acquis par l'abonné ainsi qu'une indication de fonction de maître M ou d'esclave S dont le rôle est expliqué ci-dessous. Ce tableau 17 peut aussi être utilisé pour mémoriser d'autres informations, dites informations de service, comme cela est également expliqué ci-dessous. Les produits P, c'est-à-dire notamment les événements que l'abonné est autorisé à visionner, peuvent être liés aux contrats d'abonnement ou aux modules de sécurité. Cela signifie que les produits peuvent être les mêmes pour tous les modules de sécurité d'un abonné ou au contraire, peuvent être différents pour des modules différents. Ainsi, il est par exemple possible de limiter les produits accessibles à partir d'un ensemble décodeur/module de sécurité déterminé. Ces produits peuvent être des canaux, des bouquets, des événements comme cela est bien connu de l'homme du métier. L'étape de recherche d'informations et de création de liens dans la base de données porte la référence 23 sur la figure 2a.

- [42] La clé de chiffrement U_k liée au numéro unique SN_d du décodeur STB1 doit encore être transmise au module de sécurité ICC1 de façon à pouvoir chiffrer les communications entre ce module de sécurité et le décodeur. L'envoi de cette clé est généralement effectué dans un message de gestion EMM chiffré au moyen d'une clé privée globale de l'opérateur, qui est la même pour tous les modules de sécurité gérés par cet opérateur. Le décodeur associé au module de sécurité auquel est destiné ce message peut le recevoir et le transmettre au module de sécurité qui déchiffre le

message au moyen de la clé publique globale de l'opérateur et en extrait la clé d'appariement U_k . Cette clé d'appariement est stockée dans une mémoire du premier module de sécurité ICC1 avec le numéro unique du décodeur SN_d . L'étape d'appariement porte la référence 24 sur la figure 2a. Dans une étape ultérieure 25, les droits de déchiffrement des produits P tels que déduits du tableau 17 de la base de données sont chargés dans le module de sécurité.

[43] La base de données du centre de gestion attribue au module de sécurité lié à ce premier décodeur, une fonction de maître M, ce qui est représenté par la référence 26 sur la figure 2a.

[44] Lorsque toutes les données ont été introduites dans la base de données et que la clé d'appariement U_k a été transmise au module de sécurité, le décodeur STB1 doit être activé, pour permettre le décodage, comme cela est illustré dans l'étape 27. Le centre de gestion envoie ensuite une 'commande décodeur' à destination du décodeur considéré STB1. Une 'commande décodeur' est une commande destinée au décodeur, transmise sous forme de message d'autorisation EMM, et traitée par le module de sécurité du fait que le décodeur ne dispose pas des moyens de sécurité suffisants pour traiter directement cette commande. Le message d'autorisation EMM est transmis sous forme chiffré au moyen de la clé globale de l'opérateur. Ce message est déchiffré par le module de sécurité au moyen de la clé globale. Comme le module de sécurité peut déterminer que cette commande ne le concerne pas, il le chiffre au moyen de la clé d'appariement U_k , puis le renvoie au décodeur qui le déchiffre et applique la commande.

[45] Cette 'commande décodeur' contient des données d'identification du module de sécurité maître, ces données étant généralement son numéro d'identification SN_M ou pouvant être d'autres données permettant d'identifier le module de sécurité, et une valeur de désactivation qui est généralement une valeur temporelle. Les données d'identification sont mémorisées dans la mémoire du décodeur et la valeur de désactivation est attribuée à un compteur du décodeur. Il est à noter que dans l'exemple décrit, le numéro d'identification SN_M du module de sécurité maître est égal au numéro d'identification du premier module de sécurité SN_1 puisque ce premier module de sécurité a la fonction de maître.

[46] A ce stade, le décodeur demande le numéro unique SN_d du module de sécurité et le compare avec celui reçu dans le message contenant la 'commande décodeur'. Si ces valeurs sont égales, ce qui est bien entendu le cas si le module d'origine n'a pas été remplacé par un autre module, le décodeur agit sur les moyens de désactivation de façon à débloquent le transfert des messages de contrôle ECM des événements vers le module de sécurité et les mots de contrôle peuvent être déchiffrés. Le compteur du décodeur est également activé. Si l'abonné n'a qu'un seul décodeur et qu'un seul module de sécurité, ceux-ci fonctionnent de manière appariée, comme cela est décrit dans la demande WO 99/57901, et le déchiffrement des événements chiffrés se

fait de façon conventionnelle.

- [47] Dans la description ci-dessus, les échanges entre le module de sécurité et le décodeur se font de façon chiffrée au moyen de la clé d'appariement U_k1 . Il est toutefois possible de prévoir que ces échanges sont chiffrés au moyen d'une clé de session, qui est différente de la clé d'appariement, mais qui en découle.
- [48] Lorsque l'abonné souhaite acquérir un deuxième décodeur, il doit bien entendu acquérir un deuxième module de sécurité. La mise en service du deuxième décodeur est représentée dans son ensemble par la figure 2b. L'acquisition d'un deuxième décodeur STB2 et d'un deuxième module de sécurité ICC2 est représentée par la référence 30. Comme précédemment, l'abonné doit appeler le centre de gestion CG et indiquer les données d'identification et en particulier les numéros uniques SN_d2 et SN_M2 du deuxième décodeur STB2 et du deuxième module de sécurité ICC2, le numéro de l'abonnement C1 et éventuellement son nom Sub1 pour vérification, dans une étape 31 de la figure 2b. Les informations nécessaires sont recherchées dans la base de données dans une étape 32 et la base de données est complétée, comme cela est expliqué en référence à la figure 2a. La base de données permet de retrouver la clé d'appariement U_k2 qui est mémorisée dans le décodeur STB2. Cette clé d'appariement U_k2 est associée dans la base de données au numéro unique SN_d2 du deuxième décodeur STB2. Cette clé d'appariement U_k2 est envoyée, dans une étape 33, au deuxième module de sécurité ICC2 de façon à permettre une communication chiffrée entre le module de sécurité et le décodeur. La liste des produits est également envoyée au deuxième module de sécurité ICC2 par le centre de gestion, lors d'une étape 34. Dans la base de données du centre de gestion, une fonction d'esclave S est attribuée au deuxième module de sécurité ICC2 dans une étape 35. Comme précédemment, une 'commande décodeur' est envoyée au deuxième décodeur sous forme de message d'autorisation EMM chiffré, cette commande contenant une valeur de désactivation ainsi que le numéro d'identification SN_M du module de sécurité maître. Ceci correspond à l'étape 36 de la figure 2b. Comme précédemment, ces deux informations sont mémorisées dans le décodeur, les données d'identification étant mémorisées dans la mémoire et la valeur de désactivation étant attribuée à un compteur de ce décodeur.
- [49] A ce stade, le décodeur et son module de sécurité ne sont pas activés, de sorte que le déchiffrement d'événements chiffrés diffusés par l'opérateur n'est pas encore autorisé. Le décodeur et le module de sécurité ayant une fonction d'esclave, ils doivent être activés par le module de sécurité maître ICC_M, qui, dans l'exemple ci-dessus, correspond au premier module de sécurité ICC1. Pour ceci, un message est affiché à destination de l'abonné, pour lui demander d'insérer le premier module de sécurité ICC1 ou module de sécurité maître ICC_M dans le deuxième décodeur STB2 ou décodeur esclave S. Ceci est représenté par la référence 37 sur la figure 2b. En même temps ou après l'affichage du message, le décodeur envoie une commande au module de sécurité qu'il contient, visant à obtenir le numéro d'identification SN_d de ce module.

Ce numéro est comparé, par des moyens pour comparer les données d'identification, au numéro d'identification du module de sécurité maître SN_M provenant du centre de gestion CG et mémorisé dans le deuxième décodeur. Si ces deux numéros concordent, le décodeur active le processus de traitement du flux et met en fonction le compteur de ce décodeur. Il affiche également un message à destination de l'utilisateur, lui demandant de réintroduire le deuxième module de sécurité ICC2 dans le deuxième décodeur STB2. Lorsque ceci est fait, les moyens de désactivation sont enclenchés de telle façon que les données de télévision à péage peuvent être traitées et les événements peuvent être visionnés. L'activation du deuxième décodeur STB2, représentée par la référence 38, est alors terminée.

[50] Dans le cas où l'abonné acquiert un troisième ou un $n^{ème}$ décodeur, les opérations se déroulent comme pour le deuxième décodeur. L'abonné s'identifie auprès du centre de gestion CG, indique le numéro unique SN_d du décodeur et le numéro unique SN_s du module de sécurité associé. Ces éléments sont enregistrés comme esclaves S. L'appariement entre le module de sécurité esclave et le décodeur est effectué de façon conventionnelle, de même que le chargement des produits P.

[51] Le décodeur mémorise ensuite une valeur temporelle et le numéro d'identification unique SN1 du module maître contenu dans la 'commande décodeur' transmise par le centre de gestion. Cette valeur peut être différente pour chaque paire module de sécurité/décodeur ou être la même pour certains d'entre eux ou pour tous. A ce stade, le décodeur esclave STBn demande le numéro unique du module de sécurité. Si ce numéro est celui du maître, le décodeur est activé. Pour permettre de visionner les événements, il est toutefois nécessaire de réintroduire le module de sécurité esclave correspondant dans le décodeur.

[52] Il est à noter que dans la description, il est supposé que le premier module de sécurité est également le module de sécurité maître, ce qui est bien entendu vrai lorsque l'abonné ne dispose que d'un seul ensemble décodeur/module de sécurité. Par contre, lorsqu'il dispose de plusieurs décodeurs, le premier d'entre eux peut être enregistré comme maître par défaut, mais il est possible de décider d'attribuer à n'importe quel autre décodeur, cette fonction de maître. Pour ceci, la demande doit être faite auprès du centre de gestion qui va donc adapter les paramètres dans la base de données, dans les modules de sécurité affectés et dans tous les décodeurs. Seul un module de sécurité d'un abonné déterminé se voit attribuer la fonction de maître, tous les autres modules de sécurité étant considérés comme esclave.

[53] En suivant les procédures expliquées ci-dessus, les différents ensembles décodeur/module de sécurité de l'abonné permettent de déchiffrer et de visionner des événements de télévision à péage. La valeur temporelle de désactivation mémorisée dans un compteur de chaque décodeur est utilisée pour gérer les moyens de désactivation et pour empêcher le déchiffrement selon certains critères, en particulier après un certain temps.

- [54] Dans un premier exemple de réalisation, il est supposé que la valeur temporelle de désactivation corresponde à une durée, par exemple 30 jours. Le décodeur est donc désactivé après cette durée de 30 jours. La valeur de désactivation est mémorisée dans le compteur de chaque décodeur.
- [55] En fonctionnement normal, c'est-à-dire lorsque le module de sécurité est introduit dans le décodeur correspondant, la valeur du compteur mémorisée dans le décodeur est décrémentée à intervalles réguliers, par exemple chaque jour ou chaque heure, d'un nombre d'unités tel que le compteur atteigne une valeur nulle lorsque la durée prédéterminée est écoulée. Il est aussi possible de prévoir que le compteur est incrémenté jusqu'à ce qu'il atteigne une valeur prédéterminée. Ceci est illustré par la figure 3. Dans cette figure, il est supposé que le module de sécurité ICC1 est le module maître et que le module ICC2 est esclave. Les décodeurs STB1 et STB2 sont respectivement associés aux modules ICC1 et ICC2. Dans une étape 40, le décodeur interroge à intervalles réguliers, le module de sécurité qu'il contient pour déterminer son numéro d'identification SN₁. Si ce numéro est égal au numéro d'identification du deuxième module de sécurité SN₂, il est vérifié, dans une étape 41, si la valeur du compteur est nulle. Si ce n'est pas le cas, le compteur du deuxième décodeur est décrémenté selon une règle prédéfinie. Ceci est réalisé dans une étape 42 de la figure 3.
- [56] Si cette valeur de compteur est nulle ou a atteint une valeur prédéterminée, ce qui est illustré par la référence 43, les moyens de désactivation sont utilisés de telle façon que l'abonné ne puisse plus visionner les événements. Dans le cadre des moyens de désactivation, plusieurs possibilités peuvent être mises en œuvre pour désactiver l'accès aux données de télévision à péage. Il est possible de forcer le décodeur à bloquer la transmission des messages de contrôle ECM contenant les données relatives aux événements vers le module de sécurité, de sorte que ces messages n'arrivent pas au module de sécurité. Il est également possible de forcer le décodeur à ne pas recevoir les mots de contrôle déchiffrés envoyés en retour par le module de sécurité. Une autre possibilité consiste à bloquer la transmission du son et des images provenant du module de désembrouillage du décodeur. Dans ce cas, le déchiffrement est effectué normalement, mais l'utilisateur ne reçoit rien sur son écran de téléviseur. Dans tous les cas, c'est le décodeur qui est en charge du blocage de l'affichage des événements.
- [57] Lorsque la valeur du compteur est nulle ou a atteint une valeur prédéfinie, il est nécessaire de réactiver l'ensemble pour permettre le déchiffrement des événements. Il est à noter que selon le mode de réalisation, il n'est pas nécessaire d'attendre que la valeur soit nulle pour réactiver l'ensemble. Il est possible d'effectuer une réactivation plus rapidement, de façon à réinitialiser la valeur du compteur et éviter ainsi sa mise à zéro. A cet effet, le décodeur peut disposer de moyens pour indiquer l'avancement de ce compteur.
- [58] La réactivation d'un décodeur désactivé du fait que le compteur a atteint une valeur

nulle se passe de la façon suivante. Supposons que le compteur du deuxième décodeur STB2 ait atteint une valeur nulle ou une valeur prédéfinie de sorte qu'il est désactivé. Le module de sécurité ICC2 apparié au décodeur désactivé est retiré de ce décodeur. Le module de sécurité maître ou premier module de sécurité ICC1, est introduit dans ce décodeur dans une étape 44 de la figure 3. Le décodeur esclave STB2 envoie une commande en vue d'obtenir le numéro d'identification unique du module de sécurité qui est dans ce décodeur. Celui-ci vérifie ensuite, par les moyens de comparaison, si le numéro d'identification unique SN_N du module de sécurité maître est identique au numéro d'identification SN_M que le décodeur a mémorisé lors de son initialisation. Ceci est effectué dans une étape 45 de la figure 3. Si ces numéros correspondent, le compteur du décodeur est réinitialisé dans une étape 46 et une nouvelle valeur temporelle de désactivation est introduite dans ce compteur. Cette valeur de désactivation est généralement la valeur mémorisée dans le décodeur. Il est à noter que la valeur mémorisée dans le décodeur peut être modifiée au moyen d'un message d'autorisation EMM envoyé par le centre de gestion. Dans ce cas, la nouvelle valeur mémorisée dans le décodeur s'applique à chaque réactivation. Elle peut également être une valeur reçue directement du centre de gestion par un message d'autorisation EMM adressé au module de sécurité. Si cette nouvelle valeur n'est pas mémorisée dans le décodeur, elle s'applique uniquement pour la réactivation en cours. Le module de sécurité maître peut ensuite être retiré et le module de sécurité esclave ICC2 apparié à ce décodeur peut être réintroduit pour décoder le contenu chiffré envoyé par l'opérateur. Si le numéro d'identification du module maître ne correspond pas, le compteur n'est pas réinitialisé et les événements ne peuvent pas être visionnés. Les instructions pour l'abonné sont de préférence affichées à l'écran du téléviseur associé au décodeur désactivé de sorte que l'abonné n'a qu'à effectuer les opérations étape par étape.

[59] Dans une forme de réalisation préférée, il n'est pas nécessaire d'attendre qu'un message apparaisse sur l'écran du téléviseur pour générer la réinitialisation du compteur. Ceci peut en effet se faire à tout moment en introduisant le module de sécurité maître dans l'un des décodeurs esclaves.

[60] Selon une option, il est possible d'incrémenter le compteur 'manuellement' d'une valeur correspondant à une durée relativement courte, par exemple 2 heures. Ceci permet de laisser à l'utilisateur le temps de finir de visionner un événement en cours malgré le fait que le compteur du décodeur considéré ait atteint une valeur nulle. Selon une autre option, il est également possible d'afficher un message d'avertissement à destination de l'abonné, lui indiquant que le module de sécurité peut encore fonctionner pendant une durée relativement courte, par exemple 48 heures. Ceci peut être réalisé en déterminant, à intervalles réguliers, la valeur du compteur. L'abonné dispose donc d'un certain temps pour incrémenter le compteur en introduisant le module de sécurité maître avant que le module de sécurité ne soit désactivé.

- [61] Le premier module de sécurité associé au premier décodeur, auquel est attribué le statut de maître fonctionne de manière identique aux modules esclaves. Toutefois, comme généralement, ce premier module de sécurité est placé dans le premier décodeur, le compteur est réinitialisé à intervalles réguliers. En utilisation normale, lorsque ce compteur tombe à zéro, il est immédiatement réinitialisé par le module de sécurité maître. Le module de sécurité maître et le décodeur associé peuvent donc normalement toujours déchiffrer les événements.
- [62] Selon une variante de réalisation, le décodeur envoie à intervalles réguliers, une commande visant à obtenir le numéro d'identification unique du module de sécurité qui est introduit dans ce décodeur. Si ce numéro d'identification est celui du module maître, le compteur est réinitialisé. Dans ce cas, le décodeur lié au module maître ne tombe jamais à zéro en utilisation normale, c'est-à-dire lorsque le module de sécurité maître est placé dans le décodeur correspondant.
- [63] Cette variante est avantageuse également pour l'utilisateur de decodeurs liés à des modules de sécurité esclaves puisqu'elle permet de réinitialiser un compteur à tout moment, quelle que soit la valeur réelle contenue dans le compteur. Dans ce cas, il est possible de laisser le module de sécurité maître dans l'un des decodeurs liés à un module esclave jusqu'à ce que la prochaine commande de recherche du numéro d'identification soit générée par le décodeur. Il est également possible de prévoir une activation manuelle de cette commande par l'utilisateur ou une commande automatique qui est lancée dès qu'un module de sécurité est introduit dans un décodeur.
- [64] Il est également possible de prévoir que l'intervalle entre deux commandes d'obtention du numéro d'identification soit relativement grand lorsque la valeur du compteur est élevée, puis diminue lorsque cette valeur de compteur diminue. Ainsi, si un message d'avertissement informe l'abonné que le module de sécurité maître doit être introduit dans un décodeur donné dans un délai relativement court pour éviter que le compteur ne tombe à zéro, l'abonné ne devra laisser son module de sécurité maître dans le décodeur à réinitialiser que jusqu'à ce que la prochaine commande d'obtention du numéro d'identification soit émise par ce décodeur. Cette durée peut typiquement être de l'ordre de quelques centaines de millisecondes.
- [65] Dans une autre variante de réalisation, le compteur contient une date déterminée. Le flux de données envoyé par le centre de gestion au décodeur contient un signal représentant l'heure et la date, ce signal étant connu sous l'acronyme TDT (Time & Date Table). Le décodeur esclave compare, à intervalles réguliers, la valeur du compteur à la valeur courante de la date, données par le signal TDT. Aussi longtemps que la date du compteur est postérieure à la date courante, le décodeur esclave fonctionne de façon conventionnelle, c'est-à-dire que le déchiffrement du contenu peut être réalisé.
- [66] Lorsque la date effective, envoyée par le signal TDT est postérieure ou égale à la date du compteur, le décodeur bloque le transfert des messages de contrôle ECM au

module de sécurité de sorte que le contenu des événements ne peut plus être déchiffré. Il est à noter que, comme précédemment, le compteur peut être incrémenté manuellement de quelques heures, pour éviter qu'une manipulation de mise à jour ne doive être exécutée lorsque l'abonné est en train de visionner un événement. Un message est affiché à destination de l'abonné, ce message demandant à l'abonné d'insérer le module de sécurité maître dans le décodeur esclave.

[67] Selon une variante de réalisation, le compteur comprend une valeur numérique qui correspond à un certain nombre d'impulsions temporelles. Le flux de données dans lequel sont contenus les événements comporte des informations temporelles envoyées à intervalles réguliers. Chaque fois que le décodeur reçoit une impulsion, il décrémente le compteur par exemple d'une unité. Il est également possible de faire varier l'intervalle entre deux impulsions de façon à ajuster l'intervalle entre deux réactivations.

[68] Dans ces variantes, le centre de gestion peut chiffrer les valeurs du compteur dans une 'commande décodeur' spécifiquement adressée à un module de sécurité ou à un groupe de modules. Le module de sécurité auquel cette commande est adressée déchiffre ce type de commande et la renvoie, chiffrée avec la clé d'appariement, au décodeur qui applique la commande qui lui est destinée et donc modifie la valeur du compteur en conséquence.

[69] Comme décrit précédemment, l'incrémementation du compteur des décodeurs esclaves est effectuée d'après une valeur temporelle mémorisée dans le décodeur à réinitialiser. Il est également possible d'envoyer un message d'autorisation EMM à destination d'un décodeur particulier, dans une 'commande décodeur', imposant une valeur temporelle de désactivation à ce décodeur. Dans ce cas, cette nouvelle valeur ne s'applique qu'à ce décodeur ou aux décodeurs auquel le message est destiné. Cette façon de faire permet par exemple de désactiver avec effet immédiat, un décodeur qui est suspecté d'avoir été vendu sans autorisation.

[70] Dans une deuxième forme de réalisation de l'invention, illustrée par les figures 4a et 4b, lorsque l'utilisateur acquiert un premier contrat d'abonnement de télévision à péage, C1, il acquiert également comme précédemment, un premier décodeur STB1 associé à un premier module de sécurité ICC1. L'activation de l'ensemble décodeur/module de sécurité se passe exactement comme ce qui a été décrit en référence à la figure 2a. Les références de cette figure 4a sont donc les mêmes que celles de la figure 2a.

[71] En résumé, les données liées à l'utilisateur, à son premier décodeur et son premier module de sécurité sont recherchées dans la base de données DB du centre de gestion CG. La clé d'appariement U_k 1 est transmise au module de sécurité de même que les produits et la fonction de maître. Une 'commande décodeur' contenant une valeur temporelle de désactivation ainsi que le numéro d'identification du module de sécurité maître est envoyée au décodeur. L'ensemble est activé de sorte qu'il est possible de

déchiffrer des données et de visionner des événements.

[72] Lorsque l'abonné souhaite acquérir un deuxième décodeur, il doit bien entendu acquérir un deuxième module de sécurité. La mise en service du deuxième décodeur est représentée dans son ensemble par la figure 4b. Dans une première partie du procédé, à savoir dans les étapes portant les références 30 à 36, cette mise en service se déroule de façon identique à ce qui a été décrit en référence à la figure 2b. L'abonné appelle donc le centre de gestion, qui recherche les informations pertinentes dans sa base de données. L'appariement entre le deuxième module de sécurité ICC2 et le deuxième décodeur STB2 est effectué de façon conventionnelle par la transmission au module de sécurité de la clé d'appariement U_k . Les droits associés aux produits sont également transmis comme précédemment, puis une 'commande décodeur' contenant une valeur temporelle de désactivation et le numéro d'identification du module de sécurité maître est envoyée au décodeur.

[73] L'étape 47 suivante diffère de l'étape décrite dans le mode de réalisation de la figure 2b. En effet, dans cette étape 47, on réalise un appariement entre le module de sécurité maître ICC_M ou premier module de sécurité ICC1 et le deuxième décodeur STB2. Pour ceci, un message est affiché à destination de l'abonné, pour lui demander d'insérer le premier module de sécurité ICC1 ou module de sécurité maître M' dans le deuxième décodeur STB2 ou décodeur esclave S. Durant cette phase d'activation, le centre de gestion CG envoie au module de sécurité maître un message chiffré par la clé globale de l'opérateur, ce message contenant la clé d'appariement U_k entre le deuxième décodeur STB2 et le deuxième module de sécurité ICC2. Cette clé est donc utilisée pour chiffrer les communications du deuxième décodeur STB2 aussi bien avec le premier module de sécurité ICC1 qu'avec le deuxième module de sécurité ICC2. Cette clé est stockée dans une table d'appariement mémorisée dans le module de sécurité maître.

[74] A ce stade, le décodeur esclave STB2 demande le numéro unique du module de sécurité. Si ce numéro est celui du module maître SN_M, le décodeur active le processus de traitement du flux de données et les événements peuvent être visionnés. L'activation du deuxième décodeur STB2, représentée par la référence 47, est alors terminée. Il est à noter que pour visionner un événement, il faut réintroduire le deuxième module de sécurité ICC2 dans le deuxième décodeur STB2, ce qui correspond à une étape 48 de la figure 4b. Il est envisageable de laisser la possibilité au module de sécurité maître de déchiffrer des événements à partir de n'importe quel décodeur, mais en pratique, cela n'est pas souhaité. Le déchiffrement est généralement autorisé lorsqu'un décodeur est associé à un seul module de sécurité et inversement.

[75] Dans le cas où l'abonné acquiert un troisième ou un n^{ième} décodeur, les opérations se déroulent comme pour le deuxième décodeur. L'abonné s'identifie auprès du centre de gestion CG, indique le numéro unique SN_d du décodeur et le numéro unique SN_s du module de sécurité associé. Ces éléments sont enregistrés comme esclaves S. Le

chargement des produits P et l'appariement entre le $n^{\text{ième}}$ décodeur STBn et le $n^{\text{ième}}$ module de sécurité ICCn sont effectués de façon conventionnelle au moyen d'une clé d'appariement U_k . Un appariement est ensuite réalisé entre le décodeur considéré STBn et le module de sécurité maître ICC_M ou premier module de sécurité ICC1, au moyen de la clé d'appariement U_k . Le décodeur mémorise ensuite une valeur temporelle et le numéro d'identification unique SN1 du module maître contenu dans la 'commande décodeur' transmise par le centre de gestion dans la commande de décodeur. Cette valeur peut être différente pour chaque paire module de sécurité/décodeur ou être la même pour certains d'entre eux ou pour tous. L'activation de l'ensemble module/décodeur est réalisée au moyen du module de sécurité maître. Le déchiffrement des événements est possible lorsque le $n^{\text{ième}}$ module de sécurité ICCn est de nouveau introduit dans le $n^{\text{ième}}$ décodeur STBn.

- [76] La désactivation des décodeurs, dans ce mode de réalisation, se passe de manière identique à ce qui a été expliqué en référence aux figures 2a et 2b.
- [77] Pour l'essentiel, la réactivation d'un décodeur est similaire dans le mode de réalisation décrit par les figures 4a et 4b et dans celui décrit par les figures 2a et 2b. Toutefois, dans celui des figures 4a et 4b, le décodeur ne se contente pas de vérifier le numéro d'identification unique du module de sécurité maître. On effectue en effet une véritable authentification de ce module. Différentes méthodes d'authentification sont possibles. L'une d'elles est décrite ci-dessous. Le décodeur esclave, par exemple STB2, génère un nombre aléatoire qu'il envoie en clair au module de sécurité maître, par exemple ICC1. Celui-ci le chiffre avec la clé d'appariement U_k destinée à chiffrer les communications entre ce décodeur STB2 et le module maître ICC1. Il renvoie ensuite le nombre chiffré au décodeur STB2 qui le déchiffre avec la clé d'appariement U_k et le compare au nombre initial. Parallèlement, une authentification en sens inverse peut également être réalisée. Dans ce cas, le module de sécurité maître génère un nombre aléatoire, l'envoie en clair au décodeur qui le chiffre avec la clé d'appariement U_k et le renvoie au module de sécurité. Celui-ci le déchiffre et le compare au nombre initial. Si la comparaison indique que les deux valeurs sont identiques, le compteur est réinitialisé et il est de nouveau possible de visualiser les événements. Dans le cas contraire, le traitement des données n'est pas autorisé.
- [78] Ce mode de réalisation permet d'assurer une meilleure sécurité contre l'utilisation induite d'un module de sécurité incorrect.
- [79] Les figures 5, 6a et 6b décrivent un mode de réalisation particulier dans lequel l'abonné dispose d'un module de sécurité supplémentaire par rapport au nombre d'ensembles décodeur/module de sécurité.
- [80] Comme cela est illustré par la référence 60 sur la figure 6a, un utilisateur de services de télévision à péage doit tout d'abord acquérir un contrat C1. Lorsque l'abonné acquiert un premier décodeur STB1, il acquiert également, comme précédemment, un premier module de sécurité ICC1, ce qui est représenté par une

étape 62 sur la figure 6a. En même temps que l'abonnement, il acquiert en outre, lors d'une étape 61, un module de sécurité supplémentaire, dénommé 'module contrat' ICC_c . Selon une réalisation avantageuse, ce module contrat peut être facilement distingué des autres modules de sécurité, par exemple en utilisant une couleur différente, comme cela est représenté par la figure 5.

[81] Comme dans le mode de réalisation précédent, le centre de gestion CG contient une base de données ayant le numéro d'identification unique SN_d des décodeurs et une clé d'appariement U_k associé à ce numéro. Au cours d'une étape 63 sur la figure 6a, lorsqu'un nouvel abonné appelle le centre de gestion pour initialiser son décodeur, il devra indiquer un numéro d'identification unique SN_c du module contrat, un numéro d'identification unique SN_s du premier module de sécurité, un numéro d'identification du décodeur SN_d et un numéro du contrat. Ces indications permettront de lier les données attachées au module de sécurité aux données attachées au décodeur dans la base de données. Cette étape porte la référence 64.

[82] Lorsque ces indications ont été introduites dans la base de données, il est demandé à l'abonné d'introduire le premier module de sécurité ICC1 dans le décodeur STB1. Ceci correspond à la référence 65. Lorsque ceci est fait, le centre de gestion envoie un message d'appariement et un message d'initialisation. Le message d'appariement contient la clé d'appariement U_k 1 entre le premier décodeur STB1 et le premier module de sécurité ICC1. Le message d'initialisation contient une valeur temporelle de désactivation ainsi que le numéro d'identification unique ICC_c du module contrat. La valeur de désactivation est mémorisée dans le premier décodeur. Les droits relatifs aux produits P que l'abonné est autorisé à déchiffrer sont ensuite chargés dans le premier module de sécurité au cours d'une étape 66.

[83] Lorsque ces indications ont été introduites dans la base de données, il est demandé à l'abonné d'introduire le module contrat ICC_c dans le premier décodeur STB1, ce qui correspond à une étape 67. Ce module contrat et ce premier décodeur sont alors appariés, au moyen de la clé d'appariement U_k 1 mémorisée dans la base de données, cette clé permettant d'apparier d'une part le premier décodeur STB1 avec le premier module de sécurité ICC1 et d'autre part, le premier décodeur STB1 avec le module de sécurité contrat ICC_c . Cet appariement est effectué de la même façon que décrit précédemment. Il est à noter qu'en règle générale, le module contrat ne permet pas de déchiffrer un contenu chiffré. Lorsque l'appariement entre le module de sécurité et le premier décodeur est terminé, il est demandé à l'utilisateur d'introduire de nouveau le premier module de sécurité ICC1 dans ce décodeur. Une commande d'activation est envoyée sous la forme d'une 'commande décodeur' à ce premier décodeur STB1 lors d'une étape 68, pour activer le premier ensemble décodeur/module de sécurité et permettre ainsi le déchiffrement des événements. Le premier module de sécurité ICC1 doit encore être introduit dans le décodeur lors d'une étape 69, pour permettre le traitement des données.

- [84] Lorsque l'abonné acquiert un deuxième décodeur STB2 associé à un deuxième module de sécurité ICC2, comme illustré par la référence 70 sur la figure 6b, il doit contacter le centre de gestion lors d'une étape 71. Au cours d'une étape 72, les données liées à l'abonné et à l'ensemble décodeur/module de sécurité sont mises à jour. Le deuxième décodeur STB2 est ensuite apparié, lors d'une étape 73, avec le deuxième module de sécurité ICC2 de la manière décrite ci-dessus. Une 'commande décodeur' est envoyée au décodeur, cette commande contenant une valeur temporelle de désactivation, qui peut être identique ou différente de la valeur de désactivation du premier décodeur, ainsi que le numéro d'identification unique SN_c du module contrat. Les droits liés aux produits P du deuxième module de sécurité sont chargés lors d'une étape 74. Le deuxième module de sécurité est retiré du décodeur et le module contrat ICC_c y est introduit. Ces deux éléments sont appariés au moyen de la clé d'appariement U_k2 contenue dans la base de données. Cet appariement est effectué au cours d'une étape 75. La clé d'appariement entre le deuxième décodeur et le deuxième module de sécurité est la même que la clé d'appariement entre le décodeur et le module de sécurité contrat. Le compteur du deuxième décodeur est activé lors d'une étape 76.
- [85] Le module contrat est ensuite retiré du décodeur et le deuxième module de sécurité ICC2 y est de nouveau introduit dans une étape 77. A ce stade, il est possible de visionner les événements chiffrés.
- [86] La procédure d'activation d'un troisième ou n^{ième} ensemble décodeur/module de sécurité est identique à celle expliquée ci-dessus pour le deuxième ensemble.
- [87] Comme mentionné précédemment, en général, le module contrat n'est pas prévu pour pouvoir déchiffrer un contenu chiffré. Il est toutefois envisageable au contraire, de réaliser un module contrat qui soit capable de déchiffrer le contenu chiffré à partir de n'importe lequel des décodeurs appartenant à un abonné déterminé, ou de restreindre les capacités de déchiffrement à un ou plusieurs décodeurs donnés. Le choix dépend essentiellement de l'opérateur qui diffuse le contenu chiffré.
- [88] En supposant comme précédemment que la valeur temporelle de désactivation du module de sécurité est une durée d'utilisation, le compteur est décrémenté à intervalles réguliers. Lorsqu'il arrive à zéro, le déchiffrement du contenu est bloqué et un message est affiché pour l'utilisateur. Ce message indique à l'abonné qu'il doit réactiver son ensemble décodeur/module de sécurité. Pour ceci, il doit tout d'abord retirer le module de sécurité du décodeur en question, puis y introduire le module contrat ICC_M. Une authentification de ce module contrat est faite, soit en vérifiant simplement le numéro d'identification unique, soit en effectuant une véritable authentification au moyen d'un nombre aléatoire, comme décrit précédemment. La réinitialisation du compteur se fait de la même manière que celle décrite en utilisant le premier module de sécurité comme module maître.
- [89] Comme mentionné précédemment, le module de sécurité maître ICC_M ou le module contrat ICC_c contient une table de clés d'appariement. Cette table permet de

mémoriser la clé d'appariement entre le module maître et chaque décodeur d'un abonné déterminé. En dehors de ces clés, la table peut également contenir d'autres informations telles que des informations relatives aux événements 'consommés' et des informations de service. De telles informations sont respectivement illustrées par les colonnes IPPV et Serv. du tableau 17 de la figure 1. Ces colonnes représentent les informations normalement mémorisées dans les modules de sécurité, après leur transfert au centre de gestion.

- [90] Les informations relatives aux événements consommés contiennent notamment le nombre et l'identification des événements acquis par achat impulsif (connu sous l'acronyme IPPV = Impulsive pay-per-view). Actuellement, lorsque l'achat impulsif d'événements est possible, un crédit destiné à cet achat impulsif est mémorisé dans le module de sécurité. Ce crédit est décrémenté d'un montant correspondant au prix d'un événement déterminé chaque fois qu'un tel événement est acquis par achat impulsif. Lorsque le crédit initial est consommé, l'abonné doit appeler le centre de gestion et demander une réinitialisation de son crédit.
- [91] En utilisant le système selon l'invention, la gestion des IPPV peut se passer de deux manières différentes. La première manière est celle décrite ci-dessus, c'est-à-dire que l'utilisateur appelle le centre de gestion pour commander un événement. En pratique, il peut le commander en indiquant son choix à un opérateur ou il peut par exemple utiliser des touches d'une télécommande.
- [92] La deuxième manière fonctionne comme suit. Lors d'un achat impulsif, les données relatives à cet achat, c'est-à-dire en particulier l'identification de l'événement et son prix, sont mémorisées. Ils peuvent être stockés dans le module de sécurité ICC ou dans le décodeur STB. Lorsque le module de sécurité maître est introduit dans un décodeur, en particulier dans le but d'incrémenter le compteur de ce décodeur, les données, notamment mais pas exclusivement celles concernant les IPPV, sont transmises au module de sécurité maître ou contrat. Dans le cas où les données sont stockées dans le décodeur, elles peuvent être transférées directement dans ce module maître, sous forme chiffrée ou en clair. Dans le cas où les données sont mémorisées dans le module de sécurité, elles doivent tout d'abord être transférées dans une zone de mémoire tampon du décodeur. Lorsque le module de sécurité maître est introduit dans le décodeur, ces données sont introduites dans la table du module maître. Lorsque ces données ont été transférées au module maître, le compteur peut être réinitialisé.
- [93] Cette opération de 'récolte' des données par le module maître ou par le module contrat se fait de la même manière pour tous les modules esclaves. De cette façon, le module de sécurité maître contient les informations pertinentes provenant de l'ensemble des modules appartenant à un abonné déterminé. Lorsque le module de sécurité maître est introduit dans un décodeur comportant un modem connecté à une ligne de retour, que ce soit par câble ou par réseau téléphonique public, certaines données ou la totalité d'entre elles sont envoyées au centre de gestion. Généralement,

ces données sont envoyées sous forme chiffrées. Le centre de gestion disposant de toutes les clés, il peut déchiffrer aisément le contenu du message. Il est ainsi possible de connaître exactement le contenu des événements consommés par l'abonné, ceci pour chaque décodeur individuel, ce qui permet de facturer de façon globale l'ensemble des événements. Lorsque ces données ont été transmises au centre de gestion, celui-ci peut notamment connaître le montant du solde de crédit sur chaque module de sécurité. De cette façon, il peut également incrémenter ce solde de façon à permettre à l'utilisateur d'effectuer de nouveau un achat impulsif. Cela permet également de gérer avec souplesse et fiabilité, les crédits attribués à chaque abonné.

[94] La connaissance précise des événements consommés par chaque abonné et par chaque décodeur d'un abonné offre de nombreux avantages. D'une part, comme mentionné précédemment, les crédits attribués à l'achat impulsif sont très faciles à gérer. D'autre part, il est possible de réaliser toutes sortes de statistiques, telles que par exemple la durée d'utilisation de chaque décodeur pour chaque canal. Ceci permet notamment de déterminer quels sont les produits consommés et de payer des redevances en fonction de la consommation réelle et non plus basées sur des estimations. Ceci permet également de réaliser un profil précis pour chaque décodeur et ainsi, de proposer aux utilisateurs de ces décodeurs, des événements ou des produits qui correspondent à ces attentes.

[95] La table peut également contenir des informations de service. Celles-ci peuvent par exemple décrire le niveau de réception du signal, ce qui permet notamment d'envoyer une information à l'utilisateur si l'orientation de son antenne n'est pas optimale et qu'il doit contacter un technicien. Ceci permet aussi de positionner de façon précise, une antenne d'un satellite de télécommunication de façon à avoir une zone de réception optimale. D'autres informations de services peuvent par exemple décrire la durée d'utilisation d'un décodeur ou toute sorte d'autres informations qui peuvent s'avérer utiles pour obtenir un fonctionnement optimal du système et pour réaliser des statistiques, comme cela a été décrit précédemment. Les informations de service peuvent également contenir des données relatives à des versions de logiciels ou des dates de modification de ces logiciels.

[96] Ces informations sont également récoltées par le module de sécurité maître ou contrat, puis transmises au centre de gestion lorsque ce module est introduit dans un décodeur lié à un modem connecté.

[97] Lorsque le parc de décodeurs de l'abonné ne comporte pas de modem ou qu'aucun d'entre eux n'est connecté à une ligne téléphonique, il est possible de demander à l'abonné d'envoyer le module de sécurité contrat par courrier. Dans ce cas, le centre de gestion qui demande l'envoi de ce module peut s'arranger pour qu'aucune interruption des fonctions de déchiffrement ne se produise pendant toute la durée pendant laquelle ce module est hors du domicile de cet abonné. Ceci peut être réalisé en contrôlant les valeurs temporelles de désactivation et en incrémentant celles qui risquent de tomber à

zéro pendant la période où l'abonné ne dispose plus de son module contrat. Le centre de gestion peut incrémenter le crédit de l'abonné puisqu'il connaît exactement la somme qui a été consommé.

[98] Le fait de recevoir toutes les informations de tous les décodeurs enregistrés au nom d'un même abonné présente l'avantage de générer une seule facture pour les événements consommés pour chaque abonné. Ceci comporte en outre un effet dissuasif, tel que mentionné dans le but de l'invention, puisqu'un abonné qui aurait revendu son ensemble module de sécurité / décodeur à un autre utilisateur, recevrait la facture de cet autre utilisateur. De plus, dans le cas où l'achat impulsif est possible, l'abonné ne pourrait pas contrôler le volume des achats impulsifs consommés par l'autre utilisateur et se verrait attribuer les montants correspondants sur sa facture.

[99] Les figures 7a à 7d illustrent différentes architectures de décodeur qui peuvent être utilisées dans le dispositif de l'invention. Le dispositif de la figure 7a illustre un décodeur conventionnel comportant un module de décodage D interne et un module de sécurité ICC1 amovible. Cette architecture est la plus courante et correspond à la description ci-dessus.

[100] La figure 7b représente un décodeur tel qu'illustré par la figure 7a, comportant en outre un deuxième lecteur de modules de sécurité. Dans ce cas, le module de sécurité ICC1 esclave associé au décodeur peut être laissé dans le décodeur. Le deuxième lecteur quant à lui peut recevoir le module de sécurité maître ICC1 ou le module contrat lorsque ce module doit être utilisé.

[101] La figure 7c illustre un mode de réalisation dans lequel le décodeur comporte d'une part un lecteur pour un module de sécurité ICC_c et d'autre part, un module de sécurité intégré ICC1 dans le décodeur et réalisé sous la forme d'un boîtier électronique conventionnel. En fonctionnement normal, le module de sécurité intégré au décodeur est généralement utilisé. Lorsque le compteur doit être réinitialisé, le module de sécurité extérieur est utilisé. Ce module de sécurité est par définition un module contrat. Ce mode de réalisation permet également d'utiliser le module amovible lorsque le module interne n'est plus opérationnel, par exemple suite à un changement important des fonctions effectuées par ce module.

[102] La figure 7d est similaire à la figure 7c, la différence étant que le module de sécurité ICC1 interne est intégré dans l'un des circuits intégrés du module de désembrouillage D.

[103] Les fonctions du module de sécurité peuvent également être intégrée dans le module de désembrouillage D.

[104] Dans la description ci-dessus, il a été admis que le premier module de sécurité ICC1 est le module maître dans le cas où l'abonné ne dispose pas de module contrat. Dans le cas où il dispose d'un module contrat, ce dernier jouera le rôle de maître. Pour cette raison, sauf mention explicite dans le texte, le module de sécurité maître peut être l'un des modules de sécurité appariés à un décodeur, auquel a été attribuée la fonction

de maître, ou le module contrat.

Claims

[1]

1. Décodeur destiné au traitement de données de télévision à péage, ce décodeur étant associé à au moins un module de sécurité amovible au moyen de données d'identification contenues dans ledit décodeur et dans le module de sécurité, ce décodeur comportant un module de désembrouillage, le décodeur étant caractérisé en ce qu'il comporte en outre des moyens de désactivation du traitement des données de télévision à péage et un compteur agissant sur lesdits moyens de désactivation en fonction de son contenu.
2. Décodeur selon la revendication 1, caractérisé en ce qu'il comporte en outre au moins une mémoire contenant des données d'identification spécifiques d'un module de sécurité différent de celui auquel le décodeur est associé, et des moyens pour comparer les données d'identification spécifiques mémorisées dans la mémoire avec les données d'identification du module de sécurité contenu dans le décodeur, et en ce que le compteur est initialisé par les moyens pour comparer les données d'identification.
3. Décodeur selon la revendication 1, caractérisé en ce qu'il comprend une valeur de désactivation et des moyens de comparaison de cette valeur de désactivation avec le contenu dudit compteur.
4. Décodeur selon la revendication 3, caractérisé en ce que la valeur de désactivation est une durée, une date ou une valeur numérique.
5. Décodeur selon la revendication 1, caractérisé en ce qu'il comprend des moyens de réception d'une commande agissant sur le contenu dudit compteur.
6. Décodeur selon la revendication 5 connecté localement à un module de sécurité, caractérisé en ce que lesdits moyens de réception reçoivent dudit module de sécurité, une commande agissant sur le contenu dudit compteur.
7. Système de gestion de données de télévision à péage comportant au moins deux décodeurs, chaque décodeur étant associé à au moins un module de sécurité amovible au moyen de données d'identification contenues dans ledit décodeur et dans ledit module de sécurité, ces décodeurs comportant un module de désembrouillage et des moyens de désactivation du traitement des données de télévision à péage, ce système étant caractérisé en ce que les décodeurs contiennent en outre un compteur agissant sur lesdits moyens de désactivation, et en ce qu'au moins un des modules de sécurité est déclaré maître et comprend des moyens pour réinitialiser lesdits compteurs des décodeurs.
8. Système de gestion de données selon la revendication 7, caractérisé en ce que les décodeurs comportent une mémoire contenant des données d'identification relatives au module de sécurité maître et des moyens pour comparer les données d'identification mémorisées dans ladite mémoire avec les données d'identification du module de sécurité contenu dans le décodeur, et en ce que le compteur de chaque décodeur est initialisé par lesdits moyens pour comparer

lesdites données d'identification.

9. Système de gestion de données selon la revendication 7, caractérisé en ce que seul le module déclaré maître comprend les moyens de réinitialisation desdits compteurs.

10. Système de gestion de données selon la revendication 7, caractérisé en ce qu'il comporte un module de sécurité supplémentaire par rapport au nombre de décodeurs, ce module de sécurité supplémentaire étant le module déclaré maître et comprenant les moyens pour réinitialiser lesdits compteurs des décodeurs.

11. Procédé de gestion d'au moins deux décodeurs destinés au traitement de données de télévision à péage, lesdits décodeurs étant associés à un abonné et comportant des moyens de désactivation du traitement des données de télévision à péage et un compteur agissant sur lesdits moyens de désactivation, chaque abonné disposant d'au moins deux modules de sécurité amovibles pouvant être localement connectés à au moins un décodeur, ce procédé comprenant les étapes de :

- détermination d'au moins un module de sécurité maître parmi les modules de sécurité appartenant à un abonné,
- mémorisation dans chaque décodeur de l'abonné, de données d'identification du module de sécurité maître,
- désactivation par le compteur du décodeur du traitement des données selon au moins un critère prédéfini,
- réinitialisation du compteur par l'introduction du module de sécurité maître dans le décodeur désactivé.

13. Procédé selon la revendication 12, caractérisé en ce que l'étape de vérification de la conformité du module de sécurité maître comporte une étape d'authentification d'un numéro d'identification unique dudit module de sécurité au moyen d'une clé d'appariement entre ce module de sécurité maître et le décodeur à réactiver.

14. Procédé selon la revendication 11, caractérisé en ce que la désactivation du traitement des données est faite de plus par l'envoi d'un message à au moins l'un des décodeurs de l'abonné, ce message étant envoyé par un centre de gestion.

15. Procédé selon la revendication 11, caractérisé en ce que la réinitialisation du compteur est effectuée sur la base d'une valeur de désactivation mémorisée dans chaque décodeur.

16. Procédé selon la revendication 15, caractérisé en ce que ladite valeur de désactivation est transmise aux décodeurs au moyen d'une commande d'autorisation EMM.

17. Procédé selon la revendication 11, le décodeur étant connecté à un module de sécurité esclave non autorisé à réinitialiser le compteur dudit décodeur, caractérisé en ce qu'il comprend les étapes suivantes :

- mémorisation de l'activité du traitement des données de télévision à péage dans le décodeur,
- détection de l'insertion du module de sécurité maître,
- transfert des données de l'activité du traitement dans ce module de sécurité maître.

18. Procédé selon les revendications 11 ou 17, caractérisé en ce que l'on transmet les données de traitement mémorisées dans le module de sécurité maître à un centre de gestion.

19. Procédé selon la revendication 18, caractérisé en ce que l'on transmet des données de service liées à l'abonné audit centre de gestion.

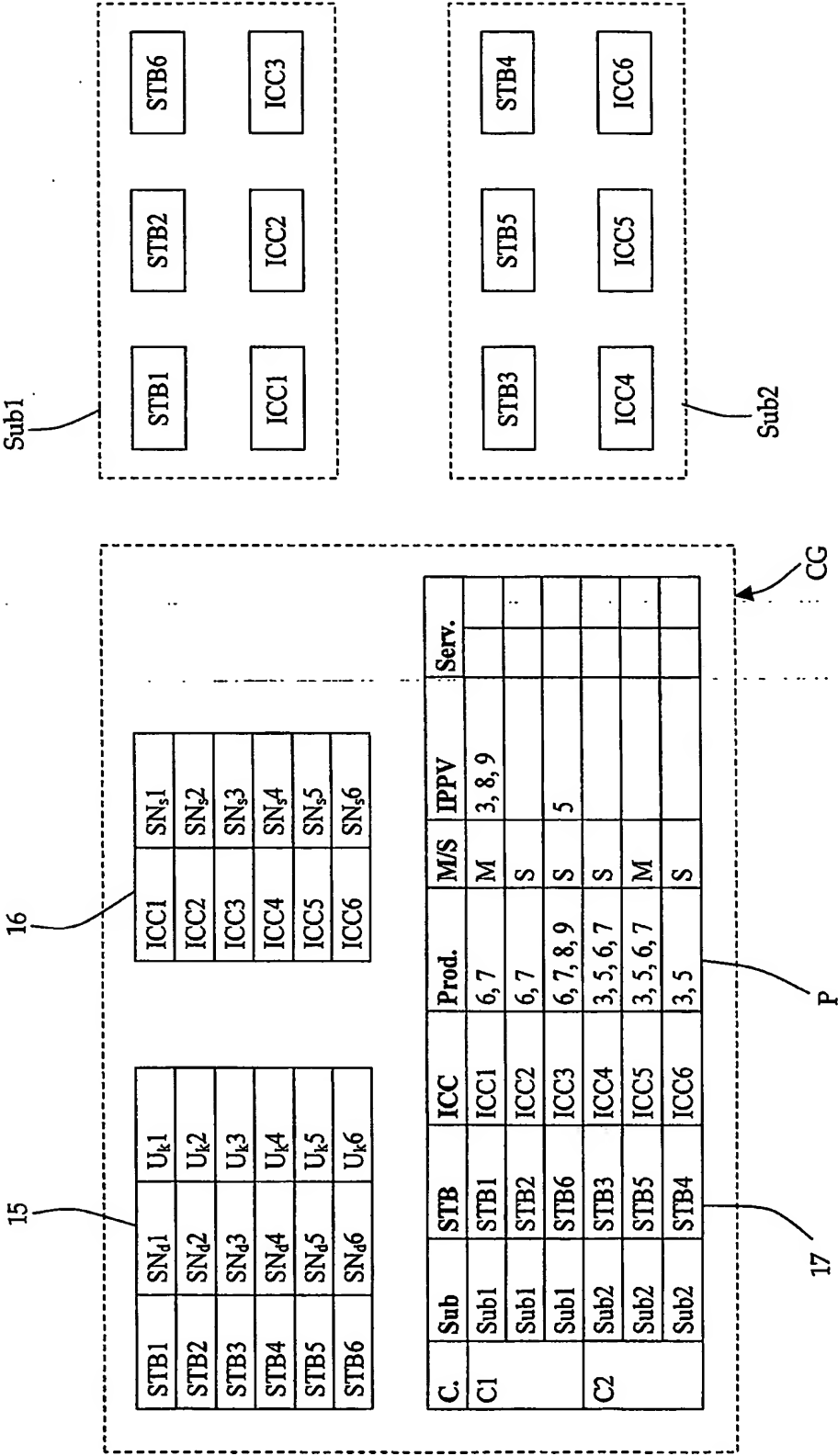


FIG. 1

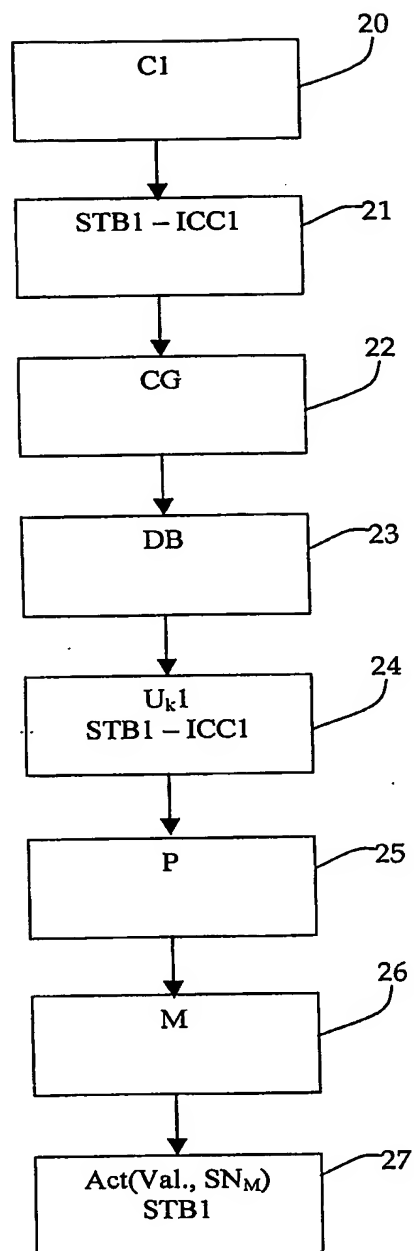


FIG. 2a

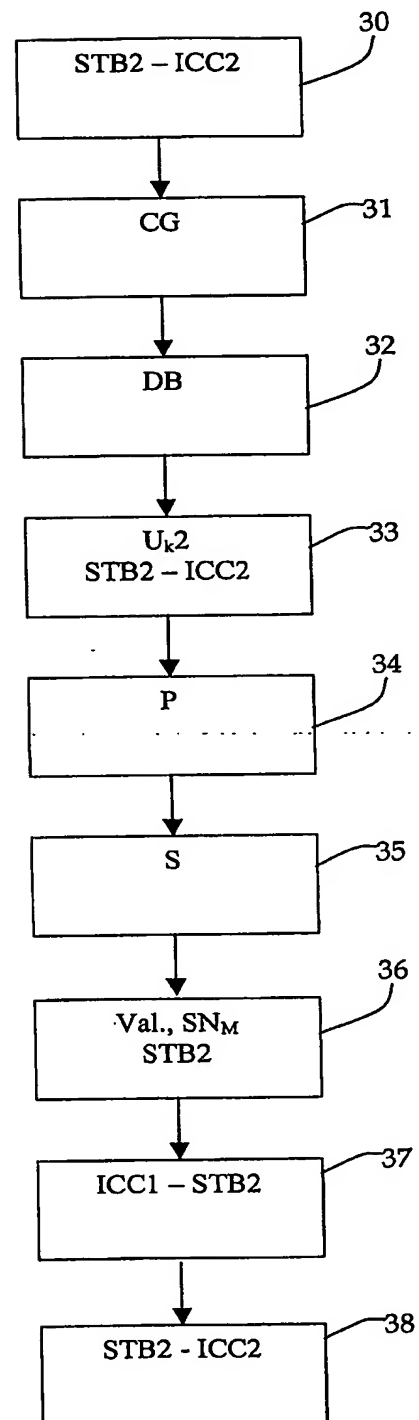


FIG. 2b

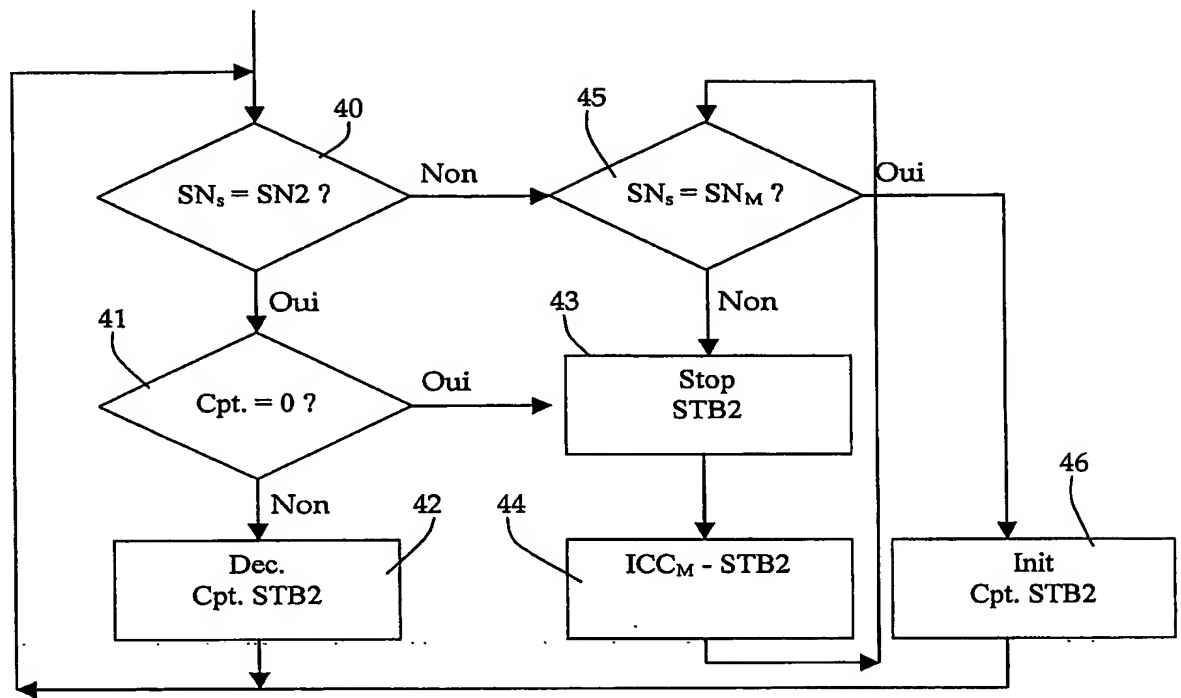


FIG. 3

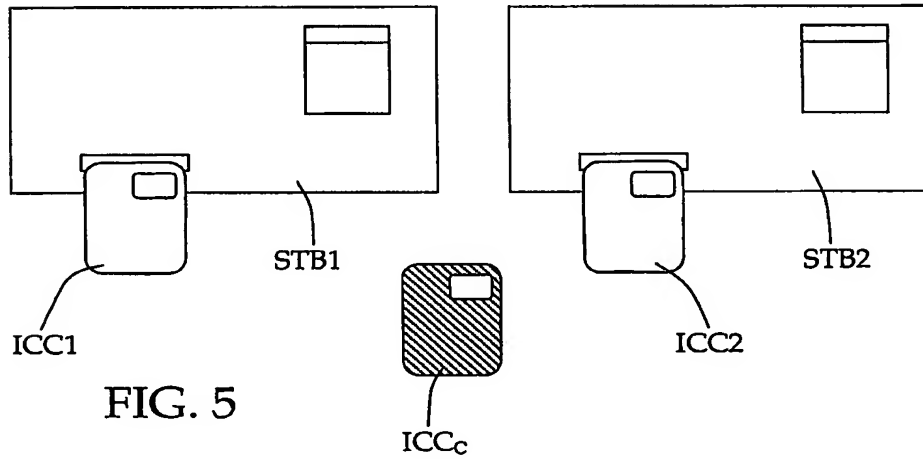


FIG. 5

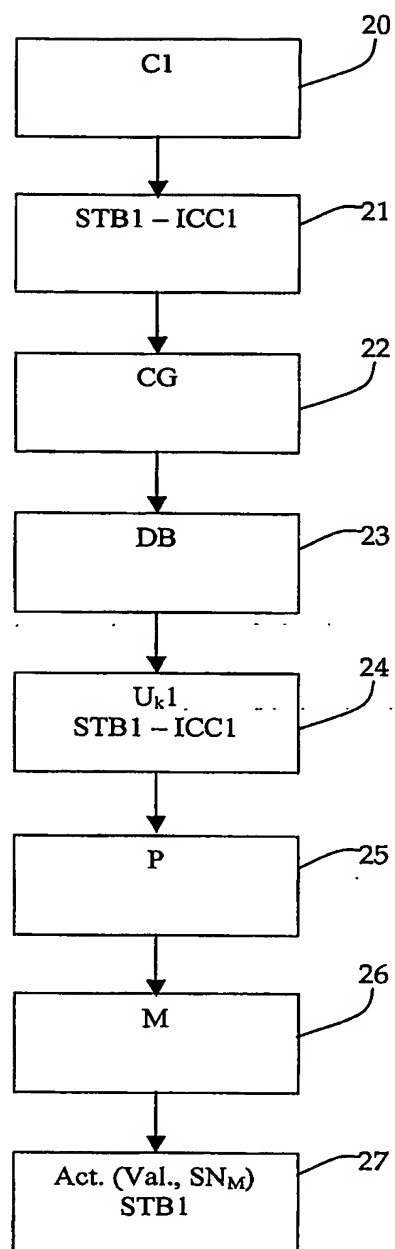


FIG. 4a

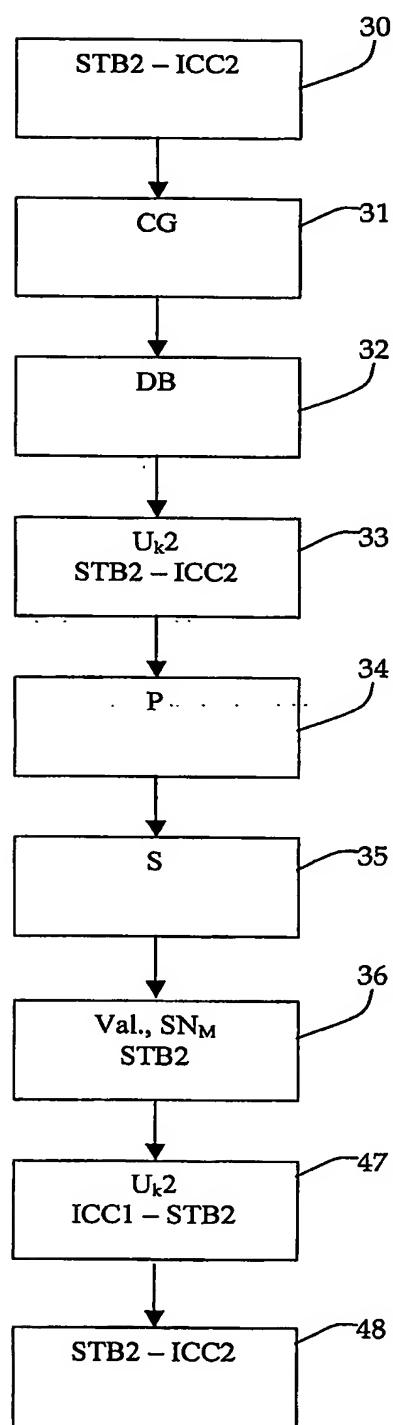


FIG. 4b

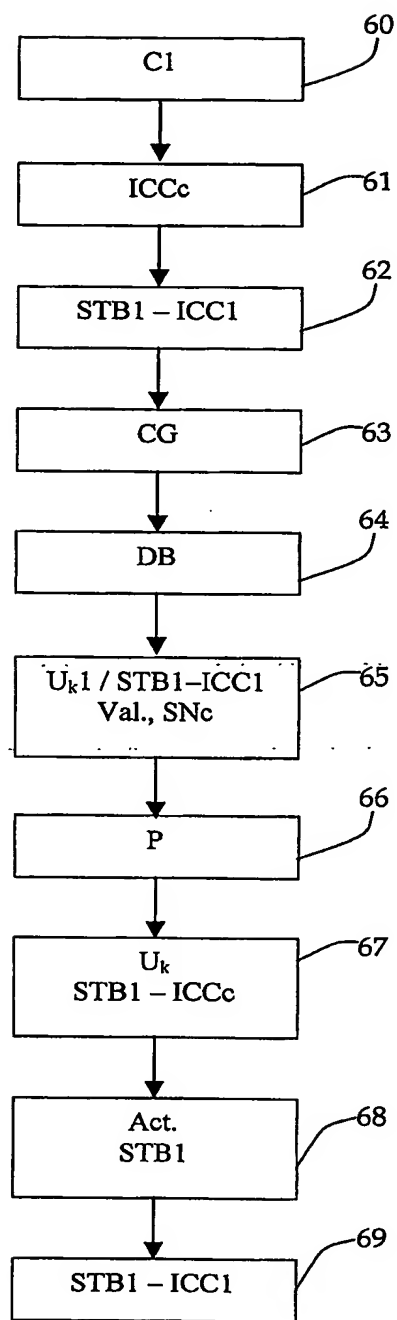


FIG. 6a

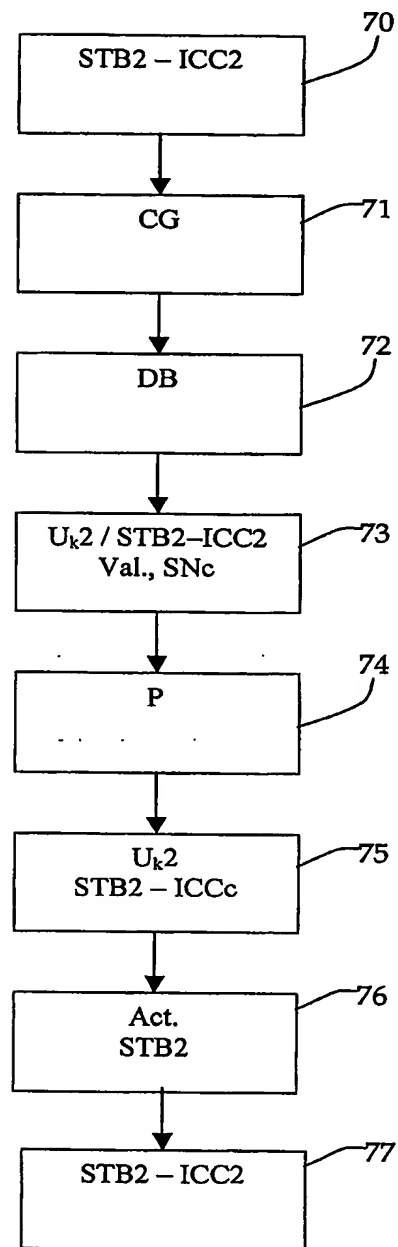
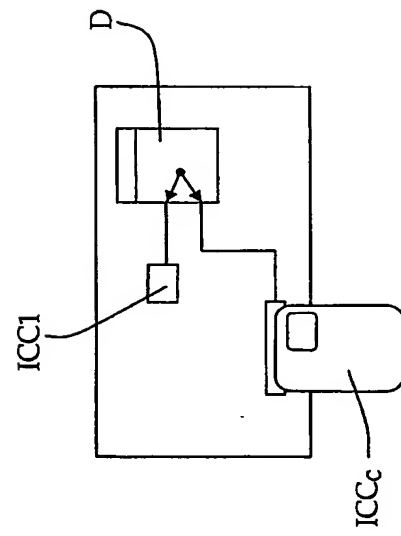
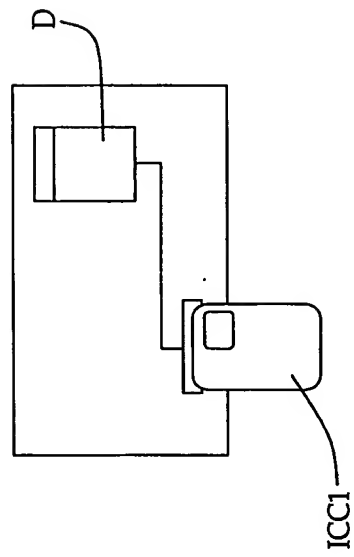
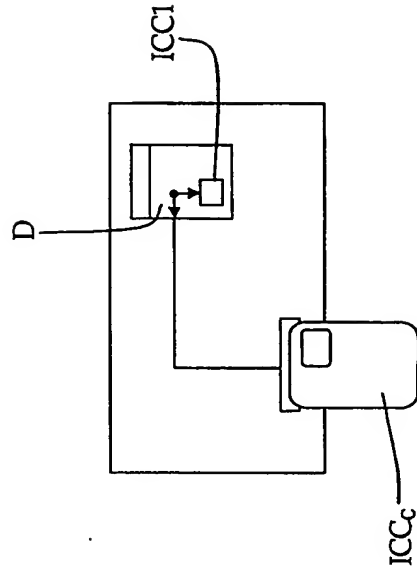
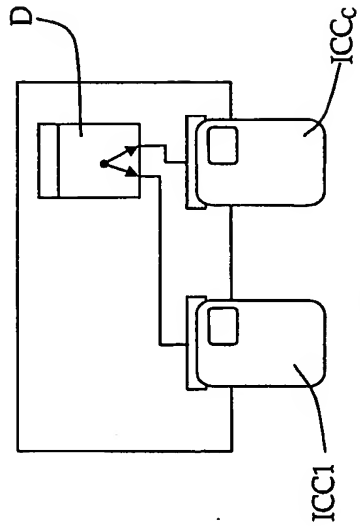


FIG. 6b



INTERNATIONAL SEARCH REPORT

International Application No. PCT/IB2004/050934

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 826 288 A (NEWS DATACOM LTD) 4 March 1998 (1998-03-04) cited in the application paragraph '0017! paragraph '0030! paragraph '0032! paragraph '0042! paragraph '0045! paragraph '0047! paragraph '0056! paragraph '0060!	1,7,11
A	US 5 748 732 A (LE BERRE JACQUES ET AL) 5 May 1998 (1998-05-05) cited in the application claim 1 <div style="text-align: center;">----- -/-</div>	1,7,11

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- *&* document member of the same patent family

Date of the actual completion of the international search

14 October 2004

Date of mailing of the international search report

05/11/2004

Name and mailing address of the ISA
 European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax: (+31-70) 340-3016

Authorized officer

Dockhorn, H

INTERNATIONAL SEARCH REPORT

ational Application No

/IB2004/050934

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>EP 0 550 959 A (ARENDS DAVID ; IBRAHIM MILAN (GB); ROSS JOHN (GB); MCGRORTY PATRICK (G) 14 July 1993 (1993-07-14) column 5, line 47 - column 6, line 15 -----</p>	11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/IB2004/050934

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0826288	A	04-03-1998	IL 117547 A	14-07-1999
			AT 196398 T	15-09-2000
			AU 1317597 A	10-10-1997
			DE 69703074 D1	19-10-2000
			DE 69703074 T2	03-05-2001
			EP 0826288 A1	04-03-1998
			ES 2151240 T3	16-12-2000
			WO 9735430 A1	25-09-1997
			JP 2001507529 T	05-06-2001
			US 6405369 B1	11-06-2002
			GB 2311451 A ,B	24-09-1997
			HK 1003410 A1	17-03-2000
US 5748732	A	05-05-1998	FR 2730372 A1	09-08-1996
			DE 69610343 D1	26-10-2000
			DE 69610343 T2	29-03-2001
			EP 0726676 A1	14-08-1996
			JP 8251569 A	27-09-1996
EP 0550959	A	14-07-1993	EP 0550959 A1	14-07-1993
			GB 2261580 A ,B	19-05-1993

RAPPORT DE RECHERCHE INTERNATIONALE

nde internationale No

PCT/IB2004/050934

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04N7/16

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 826 288 A (NEWS DATACOM LTD) 4 mars 1998 (1998-03-04) cité dans la demande alinéa '0017! alinéa '0030! alinéa '0032! alinéa '0042! alinéa '0045! alinéa '0047! alinéa '0056! alinéa '0060!	1,7,11
A	US 5 748 732 A (LE BERRE JACQUES ET AL) 5 mai 1998 (1998-05-05) cité dans la demande revendication 1	1,7,11

-/-

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- *A* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- *E* document antérieur, mais publié à la date de dépôt international ou après cette date
- *L* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- *O* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- *P* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

T document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

X document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

Y document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

Z document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

14 octobre 2004

Date d'expédition du présent rapport de recherche internationale

05/11/2004

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Dockhorn, H

RAPPORT DE RECHERCHE INTERNATIONALE

Recherche Internationale No

1/IB2004/050934

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>EP 0 550 959 A (ARENDS DAVID ; IBRAHIM MILAN (GB); ROSS JOHN (GB); MCGRORTY PATRICK (G) 14 juillet 1993 (1993-07-14) colonne 5, ligne 47 - colonne 6, ligne 15 -----</p>	11

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs

aux membres de familles de brevets

Numéro International No

PCT/IB2004/050934

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0826288	A	04-03-1998	IL 117547 A	14-07-1999
			AT 196398 T	15-09-2000
			AU 1317597 A	10-10-1997
			DE 69703074 D1	19-10-2000
			DE 69703074 T2	03-05-2001
			EP 0826288 A1	04-03-1998
			ES 2151240 T3	16-12-2000
			WO 9735430 A1	25-09-1997
			JP 2001507529 T	05-06-2001
			US 6405369 B1	11-06-2002
			GB 2311451 A ,B	24-09-1997
			HK 1003410 A1	17-03-2000
US 5748732	A	05-05-1998	FR 2730372 A1	09-08-1996
			DE 69610343 D1	26-10-2000
			DE 69610343 T2	29-03-2001
			EP 0726676 A1	14-08-1996
			JP 8251569 A	27-09-1996
EP 0550959	A	14-07-1993	EP 0550959 A1	14-07-1993
			GB 2261580 A ,B	19-05-1993